

ORIGINAL

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FILED IN OPEN COURT
U.S.D.C. Atlanta

JUN 17 2013

James N. Hatten, Clerk
By: *Amelia J. Smith*
Deputy Clerk

UNITED STATES OF AMERICA

v.

JAMES BLOCKER

Criminal Indictment

No.

1:14CR 0228

THE GRAND JURY CHARGES THAT:

COUNT 1
(Conspiracy)

1. From in or about August 2010, through on or about August 21, 2012, the exact dates being unknown, in the Northern District of Georgia and elsewhere, defendant JAMES BLOCKER did willfully, knowingly and unlawfully combine, conspire, confederate, agree and have a tacit understanding with conspirators Thomas Allen Dye, Nicholas Anthony Narbone, and Thomas Pace, and others known and unknown to the Grand Jury, to commit certain offenses against the United States, including the following: to willfully, and for purposes of commercial advantage and private financial gain, infringe copyrights by reproducing and distributing, during a one hundred and eighty (180) day period, at least ten copies of one or more copyrighted works having a total retail value of more than \$2,500 in violation of Title 17, United States Code, Section 506(a)(1)(A), and Title 18, United States Code, Sections 2319(b)(1) and 2.

Background

2. It is relevant to this Indictment that, during the time period relevant to this conspiracy:

a. Conspirator Nicholas Anthony Narbone operated an alternative online market, called "Appbucket," for the purpose of reproducing and distributing pirated copies of Android mobile device software applications (or "apps") to Appbucket subscribers in the Northern District of Georgia and elsewhere, and for purposes of commercial advantage and private financial gain by charging subscribers monthly or annual subscription fees. Conspirator Narbone also obtained, shared, and used a computer program to circumvent and remove ("crack") the apps' technological protection measures designed to control access to, or copying of, the apps, so they may be copied and uploaded to Appbucket's computer servers without permission from the copyright owners.

b. Defendant JAMES BLOCKER was primarily responsible for writing the computer code necessary to operate the original Appbucket alternative online marketplace in 2010, under the web domain "www.appbucket.net." Defendant BLOCKER helped maintain the operation of the Appbucket computer servers by setting up services and

configuring databases on the servers. Defendant BLOCKER also uploaded pirated copies of apps to Appbucket's computer servers.

c. Conspirator Thomas Allen Dye was primarily responsible for searching for and obtaining pirated copies of copyrighted Android apps for Appbucket's computer servers, cracking the apps' technological protection measures designed to control access to, or copying of, the apps, and then uploading pirated copies of the cracked apps onto Appbucket's computer servers.

d. Conspirator Thomas Pace was primarily responsible for searching for and obtaining pirated copies of copyrighted Android apps for Appbucket's computer servers as well as uploading pirated copies of those apps onto Appbucket's computer servers.

Manner and Means

3. The manner and means by which the conspiracy was carried out included, but were not limited to, the following:

a. The object of the conspirators' illegal agreement was to unlawfully obtain, reproduce, and distribute copies of copyrighted works, namely, Android mobile device apps, through an alternative online market, called "Appbucket," without permission from the software developers and other owners of these copyrighted works, who would

otherwise sell lawful copies of the apps on legitimate Android online markets for a fee to the general public.

b. It was a part of the conspiracy to obtain by various means copies of the aforementioned apps that lacked any technological protection measures controlling access to, or copying of, the copyrighted software for the apps. For example, conspirators circumvented or removed (“cracked”) such access controls or copy controls on authorized copies of the apps, and did so without permission from the copyright owners of the apps. Other conspirators reproduced and obtained over the Internet copies of apps that were already “cracked” by others – also without permission from the copyright owners. For example, conspirator Nicholas Anthony Narbone paid co-conspirator Thomas Pace to purchase authorized copies of apps from a legitimate Android marketplace so co-conspirator Thomas Allen Dye and other conspirators could then crack and copy the apps, upload pirated copies of the apps to Appbucket’s servers, and then reproduce and distribute pirated copies of the apps to Appbucket’s subscribers through www.appbucket.net – all without permission from the copyright owners.

c. It was further a part of the conspiracy to rent computer servers, including servers located in the United States and Sweden, to host one or more websites, such as “www.appbucket.net,” and to provide

digital storage for pirated copies of copyrighted apps to allow conspirators to upload, download, store, and ready pirated copies of copyrighted Android apps for distribution to Appbucket subscribers.

d. It was further a part of the conspiracy to pay for and to register Internet domain names for use by Appbucket subscribers, including www.appbucket.net.

e. It was further a part of the conspiracy to distribute pirated copies of the apps to Appbucket subscribers without authorization from the copyright owners. Through the Appbucket website, www.appbucket.net, conspirators could distribute copies of the pirated apps from Appbucket's computer servers directly to Appbucket's subscribers' Android mobile devices.

f. It was further a part of the conspiracy to establish PayPal and other bank accounts to receive the monthly and annual subscription fees paid by Appbucket subscribers. For example, between August 20, 2010 until December 17, 2010, conspirator Nicholas Anthony Narbone received \$61,763.48 in subscriptions to www.appbucket.net via the online payment processor PayPal, and between December 18, 2010 until July 26, 2011, conspirator Narbone received approximately \$20,596.00 in subscriptions to www.appbucket.net via the online payment processor Digital River.

Defendant JAMES BLOCKER and conspirator Narbone were both authorized users of Appbucket's online payment accounts. For example, defendant BLOCKER logged into Appbucket's Digital River online payment account on multiple occasions between December 3, 2010 and June 29, 2011. Likewise, between January 5, 2011 and March 9, 2011, conspirator Narbone initiated ACH transfers totaling approximately \$8733 from Appbucket's Digital River account to his personal bank account.

g. During and as a part of the conspiracy, the conspirators distributed over one million (1,000,000) copies of copyrighted apps, with a total retail value of over \$700,000, to Appbucket subscribers and others, in the Northern District of Georgia and elsewhere, all without authorization from the software developers and other copyright owners of the apps.

Overt Acts

4. In furtherance of this conspiracy, and to effect the objects and purposes thereof, defendant and his co-conspirators committed the following overt acts within the Northern District of Georgia and elsewhere, including but not limited to the following:

a. On August 10, 2010, conspirator Nicholas Anthony Narbone registered the web domain name www.appbucket.net with a domain registrar located in Sweden.

b. On or about August 11, 2010, defendant JAMES BLOCKER configured a server to utilize the www.appbucket.net web domain name and host copies of apps for Android mobile devices.

c. On or about August 12, 2010, defendant JAMES BLOCKER uploaded hundreds of megabytes of apps to the Appbucket server.

d. On August 17, 2010, conspirator Nicholas Anthony Narbone changed the business name for his PayPal account to Appbucket.

e. On August 19, 2010, conspirator Nicholas Anthony Narbone changed the email address associated with his PayPal account from nnarbone@gmail.com to support@appbucket.net.

f. On or about August 26, 2010, conspirator Nicholas Anthony Narbone provided defendant JAMES BLOCKER a list of Appbucket subscribers to delete. Defendant BLOCKER confirmed that he would take care of deleting the subscribers.

g. Between June 22, 2010 and December 5, 2010, conspirator Nicholas Anthony Narbone sent defendant JAMES BLOCKER approximately \$7,222.00 via the Appbucket PayPal account.

h. Through on or about December 11, 2010, conspirator Nicholas Anthony Narbone sent \$11,269.00 from Appbucket's PayPal account to co-conspirator Thomas Pace, in part for the purchase of authorized copies of

apps from a legitimate Android marketplace and for the purpose of making pirated copies of those apps.

i. Between on or about August 2010 and December 11, 2010, conspirator Thomas Pace purchased apps from the Google marketplace, made pirated copies of these apps, and uploaded them to Appbucket's computer servers.

j. On various dates in December, 2010, defendant JAMES BLOCKER configured the layout for receipts generated by eSellerRate for subscriptions to www.appbucket.net.

k. On December 25, 2010, defendant JAMES BLOCKER composed and sent a system wide email to Appbucket subscribers providing them with subscription information and descriptions of new system features being implemented.

l. On January 3, 2011, conspirator Nicholas Anthony Narbone provided a signed document to eSellerRate authorizing deposits of proceeds from Appbucket's subscriptions to a Wachovia bank account in the name of conspirator Nicholas Anthony Narbone.

m. On March 10, 2011, utilizing the email account dev@appbucket.net, defendant JAMES BLOCKER sent an email to both the operator and the computer coder of a competing digital online

marketplace, called Applanet, as part of a proposed merger between Appbucket and Applanet. The email contained a link to www.appbucket.net/applanet with a username and password to access a web based administration front end for a database server.

n. On April 26, 2011, conspirator Nicholas Anthony Narbone emailed defendant JAMES BLOCKER setting forth the goals for the merger between Appbucket and Applanet.

o. On May 6, 2011, defendant JAMES BLOCKER emailed conspirator Nicholas Anthony Narbone about creating a rift between the operator and computer coder for Applanet so Appbucket could take over Applanet's userbase.

p. On July 13, 2011, defendant JAMES BLOCKER provided his bank account information to conspirator Nicholas Anthony Narbone for the purpose of receiving wire transfers.

q. On August 9, 2011, an FBI undercover employee who was also an Appbucket subscriber, in the Northern District of Georgia, downloaded 1,309 copies of pirated apps from Appbucket's computer servers.

r. On September 4, 2011, conspirator Nicholas Anthony Narbone emailed co-conspirator Thomas Allen Dye and offered to pay conspirator Dye to upload copies of apps to Appbucket's computer servers.

s. Between the dates of September 4, 2011 until on or about September 19, 2011, conspirator Thomas Allen Dye copied and uploaded pirated copies of apps to Appbucket's computer servers.

t. On September 16, 2011, conspirator Thomas Allen Dye provided bank account information to conspirator Nicholas Anthony Narbone for the purpose of getting paid for copying and uploading apps to Appbucket's computer servers.

u. On January 4, 2012, an FBI undercover employee who was also an Appbucket subscriber, in the Northern District of Georgia, downloaded 1,211 copies of pirated apps from Appbucket's computer servers.

v. On February 3, 2012, an FBI undercover employee who was also an Appbucket subscriber, in the Northern District of Georgia, downloaded 1,494 copies of pirated apps from Appbucket's computer servers.

All in violation of Title 18, United States Code, Section 371.

FORFEITURE


5. Defendant JAMES BLOCKER, if convicted of the violation alleged in count one of this indictment, shall forfeit to the United States as part of the sentencing and pursuant to Fed. R. Crim. P. 32.2:

a. any real or personal property constituting and derived from proceeds obtained directly or indirectly as a result of, or traceable to, the violation of Title 18, United States Code, Section 371, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c);


b. Any other property belonging to the defendant, up to the value of the property subject to forfeiture, if any property subject to forfeiture: (a) cannot be located upon the exercise of due diligence; (b) has been transferred to, sold to, or deposited with a third person; (c) has been placed beyond the jurisdiction of the Court; (d) has been substantially diminished in value; or (e) has been commingled with other property that cannot be subdivided without difficulty.

A Trve BILL
Idick Bass
FOREPERSON

SALLY QUILLIAN YATES
UNITED STATES ATTORNEY


CHRISTOPHER C. BLY
ASSISTANT UNITED STATES ATTORNEY
Georgia Bar No. 064634
75 Spring Street, S.W., Suite 600
Atlanta, Georgia 30303 (404) 581-6000

LESLIE R. CALDWELL
ASSISTANT ATTORNEY GENERAL


JOHN H. ZACHARIA
ASSISTANT DEPUTY CHIEF FOR LITIGATION
District of Columbia Bar No. 456867
U.S. Department of Justice, Criminal Division
Computer Crime and Intellectual Property Section
1301 New York Ave., N.W., Suite 600
Washington, D.C. 20530 (202) 305-2310